07 Jan 2010

(U) MARFOREUR G-2 TRIP REPORT[1]

(U) Traveler: Staff Sergeant Matthew Hosburgh

(U) Purpose: Chaos Communication Congress 26C3 Here Be Dragons Conference

(U) Dates: 26–30 December 2009

(U) Location: Berlin, Germany

(U) Executive Summary. The Chaos Communication Congress conference is an annual event that attracts hackers, security researchers, computer hobbyists and malicious computer users. This year's conference marked the 26th year anniversary of the congress. The conference title was *Here Be Dragons* which is a reference to medieval times where explorers would put dragons or other serpents to mark dangerous or uncharted territories--an attempt to explain the conference's purpose in exposing "uncharted territories" in computer, phone, and other systems. The conference began on 27 December 2009 and lasted until 30 December 2009. There were some good talks about security and some rather alarming developments in the "uncharted territory." A majority of the security discussions were in German which prevented attendance because of the language barrier; however, a large amount of the discussions were in English and catered to the international audience. I personally attended the following talks: Lightning Talks–Day 1; Why Net Neutrality Matters?; WikiLeaks Release 1.0; Exposing Crypto Bugs through reverse engineering; Tor and censorship: lessons learned; SCCP hacking, attacking the SS7 & SIGTRAN applications on step further and mapping the phone system; DDoS / botnet mitigation & hosting online communities; Using OpenBSC for fuzzing of GSM handsets; "Yes We Can't!"-on kleptography and cryptovirology; Black Ops of PKI.. A detailed explanation, assessment and countermeasure (if applicable) can be found below.

1. **(U) Lightning Talks – Day 1.** Lightning Talks were a two hour forum where basically members of the hacking community could present a topic or announce an event for approximately four minutes. During this talk, there were

[1] **MARFOREUR AC/S G-2 Comment**: This paper has been declassified on 05 March 2012 in accordance with the procedures set forth in DoD Instruction 5200.1-R (Information Security Program; January 1997). Prior to declassification, this paper was reviewed by the MARFOREUR AC/S G-2 (Senior Intelligence Officer), MARFOREUR AC/S G-6 (Senior Communications Officer/Chief Information Officer), USEUCOM J2 (Cyber Intelligence Division), USEUCOM Foreign Disclosure Officer, and USEUCOM SSO (INFOSEC Branch), all of whom concurred that the information contained herein does not exceed a level of UNCLASSIFIED//FOR OFFICIAL USE ONLY. The paper's author, SSgt Matthew Hosburgh, was dischared from the United States Marine Corps in June 2010 and therefore was not available to participate in this declassification review.

PROSECUTION EXHIBIT 43 for identification
PAGE OFFERED:___ PAGE ADMITTED:___
PAGE___OF___PAGES

presentations on TV-Be-Gone (a universal remote that can turn off television sets from a distance), and a few other projects that were not of much significance.

a. **(U) Analysis:** This forum seemed vary inert. There was also a lack of speakers for day one as the Internet for the conference center was down and a lot of the presentations were stored on a website on the Internet.
b. **(U) Countermeasure:** N/A

2. **(U) Why Net Neutrality Matters?** Net neutrality is fast becoming a hot topic in the information technology world. Essentially, this talk presented what it is a way for an ISP companies to more tightly regulate levels of service to the user. This could be in the form of making users pay for exactly what they need on the Internet. For example, an ISP could provide a customer with three packages to choose from, say 1 – 3. Package 1 could cost $30 per month and only allow access to Google searching and news websites. Package 2 could allow more access for $40 per month including email, web browsing, and access to banking sites. Package 3 could be the "premium package" as it would allow access to music, YouTube and other media sites (to include packages 1 – 2). The ISPs would be able to regulate the internet content and not just bandwidth. This is the core issue: limiting access to content and not bandwidth. The talk made the case the Internet should be kept open and free. Jeremie Zimmerman was the presenter (a French citizen) and he said his organization had been lobbying the French politicians to keep the Internet open. His plea to everyone at the conference was to lobby in our respective countries to keep the Internet the way it is today.

a. ~~(S//NF)~~ **(U//FOUO) Analysis:** Keeping the Internet neutral has its benefits. It allows the free exchange of ideas which promotes global communications. Basically, the Internet is the same no matter where one is in the world (relatively speaking). Taking the openness out of the Internet would hinder global communications and business. On the flipside, the Internet, as it stands today, is a playground for malicious users (creating viruses, cyber fraud, child pornography, and other crimes). Further, the Internet is an essential communication tool for terrorists. Terrorists cells can use the Internet to obscure their traffic, as well as, other tools to encrypt, hide and send messages. By filtering the Internet, this problem may be minimized, but at the cost of lost revenue and freedom of speech.
b. **(U) Countermeasure:** N/A

3. **(U) WikiLeaks Release 1.0.** Wikileaks.org, is a publicly accessible Internet Website where individuals can contact with leaked information and have it published to the public anonymously without fear of being held legally liable. The information that can be leaked includes, but is not limited to, classified information, trade secrets, corporate information, personally identifiable information, and even operational data. The goal is to promote "open-ness" and

to ensure the public is "well informed" to what's really going on. The founders of WikiLeaks claim that they have not had any of their sources compromised or uncovered. One of the most alarming pieces of the talk was that WikiLeaks was seeking to obtain "off shore" storage and data processing of their site so that they would not be bound to U.S. law. This concept is similar to that of the proverbial "Swiss bank account."

a. ~~(S//NF)~~ (U//FOUO) **Analysis**. WikiLeaks represents a potential force protection, counterintelligence, operational security (OPSEC), and information security (INFOSEC) threat to MARFOREUR/AF. The intentional or unintentional leaking and posting of US Marine Corps sensitive or classified information to Wikileaks.org poses a large threat not only from the external disclosure, but from the insider. The insider would be able to easily leak information without fear of any direct, individual, repercussions. Further, when the off-shore storage is implemented, WikiLeaks will have more latitude to distribute and publish leaked information as it will not be bound by U.S. law.

b. **(FOUO) Countermeasure:** For MARFOREUR/AF, ensure that employees are given annual security training. Remind cleared individuals of their agreement to safeguard and not disclose classified or sensitive information. Enforce document accountability. Ensure that classified information that is no longer needed is properly disposed of. Recommend implementing a control to ensure that whoever prints, the document and user is logged for all systems (unclass – SCI). Enforce the secure print feature for the printers in the hallway, that is, where uncleared individuals may be in contact with the printers.

4. **(U) Exposing Crypto Bugs through reverse engineering.** This talk was given by Philippe Oechslin of Objectif Securite. He is also a French citizen. His talk was aimed at explaining how poor coding of programs could be a way to attack a system vice trying to break the encryption algorithm. Essentially, exploiting bugs to break-in/manipulate a device or system vice trying to exploit the encryption algorithm, such as AES or 3DES. The devices he demo'd were the MXI Stealth (a FIPS 142-3 level 2 certified USB flash drive), the EISST E-Capsule (an electronic safe for data), and the Data Becker Private Safe (another electronic safe). During his demo, he showed how he could break-in to the devices, by reverse engineering the code using publically available Hex Editors and commercial tools. He used the poorly written code to obtain access to the devices.

a. ~~(S//NF)~~ (U//FOUO) **Analysis.** Based on the demonstration, standard crypto algorithms, such as, AES and 3DES are very secure if implemented correctly. They will thwart any current type of brute force attack. However, if the programmer does not implement the crypto correctly, the device or program can be exploited or access can be obtained. The crypto will remain unbroken, but the device or software can be broken because of poor implementation and reverse engineering.

b. ~~(S//NF)~~ **(U//FOUO) Countermeasure.** Ensure that USB devices, that are relied on to provide a degree of security using crypto, are certified by the NSA or other agency to ensure that they are indeed secure and free from being reverse engineered. Simply buying a "secure USB" device from the PX is not an option if it not approved. Guard the keys to decrypt the device like a password and do not write them down. Use complex passphrases to secure the device and not an easily guessable word or phrase.

5. **(U) Tor and censorship: lessons learned.** Tor is an acronym for the "The Onion Router." It is a network spread across the globe and its aim is to provide anonymity and obscurity to its users. There are seven "root" servers that are maintained by staff members of tor and other relay networks hubs that users can setup to host an instance of Tor at their location. Tor is becoming quite popular today among many censored users, for example: China and Iran. Because China and Iran block and filter content, Tor is used to circumvent these restrictions. Tor is further becoming more of a hard-to-pin-down anonymizer. Roger Dingledine was the speaker. He gave the current state of Tor in the world and how it was being utilized. Even after China attempted to block Tor, the network evolved as is still able to function despite the blockage. An alarming statement made by one of his colleagues was that "we" "should get jobs at Cisco, Symantec and other security companies to find out what their intentions are for building these security appliances (firewalls, IDS, etc) and leak them to WikiLeaks." His colleague blamed the security vendors for making it easy for governments to censor its people and thus the need to find out why and how they were going to develop the next device to make filtering easier for an organization. He further went on to say that knowing why and how they are filtering will allow "the community" to respond by catering security appliances toward organizations (businesses) and not governments for censorship.

a. ~~(S//NF)~~ **(U//FOUO) Analysis.** Tor is an effective tool that provides browser anonymity and obscurity on the Internet. It is free software available to the world. The threat it poses is that it makes it very difficult to know where certain traffic is coming from. For example, a malicious attacker could use it to obscure his or her IP address. MARFOREUR/AF's systems could be attacked by China and we would not know where they are coming from. The threat posed by this is not necessarily and insider one, it is primarily an outside threat. It would make it very difficult to monitor traffic of an individual / organization utilizing Tor.

b. ~~(C)~~ **(U//FOUO) Countermeasure.** At this point, there is not much in the way of defense as the "standard" filtering of Tor traffic can be circumvented by way of using a relay circuit within the Tor network.

Educate the users and the IA personnel on the power of Tor to hide where attacks may be coming from.

6. **(U) SCCP hacking, attacking the SS7 & SIGTRAN applications on step further and mapping the phone system.** In this talk, Philippe Langolis discussed the current state of the phone system. He said, "SS7 is like TCP/IP in the 1990s. It used to be quite a secure network because nobody outside the organizations (here, the mobile operators and telecom companies) were connected to it. Now it's getting interconnected to new actors which are not that trustworthy. He further went on to say that the Blue Box (used to generate tones which can access the "supervisory" function of the phone system. From there, additional tones can be used to generate desired effects) is making a come back. There's a world beyond pure SS7: the phone system applications themselves and most notably what transforms phone numbers into telecom addresses (also known as Point Codes, DPCs and OPCs; Subsystem Numbers, SSNs and other various fun.), and that's called Global Title Translation. Few people actually realize that the numbers they are punching on their phone are actually the same digits that are used for this critical translation function, and translate these into the mythical DPCs, SSNs and IMSIs. More and more data is now going through the phone network, creating more entry point for regular attacks to happen: injections, overflow, DoS by overloading capacities. The mobile part is opening up, thanks to involuntary support from Motorola, Apple and Android."

    a. **(U) Analysis.** The attack surface for GSM is increasing daily. With more entry points, the technology is at the tip of the security nightmare iceberg. More security problems will ensue in the next few years.
    b. **(U) Countermeasure.** N/A.

7. **(U) DDoS / botnet mitigation & hosting online communities.** This talk discussed the "business" of running an online community, such as, a social network, newsgroup, etc. The discuss honed in on what needs to happen while experiencing a Denial of Service (DoS) attack. Essentially, the speaker stressed the need to have a good relationship with the ISP or webhosting service incase something out of the ordinary should happen.

    a. **(U) Analysis.** This discussion was relatively inert; however, it does go to show that the sophistication of some of the "underground" online communities are looking at hosting as more of a business—in such to keep their communities up incase of a disaster or attack.
    b. **(U) Countermeasure.** N/A.

8. **(U) Using OpenBSC for fuzzing of GSM handsets.** More tools are available to attackers looking to exploiting the GSM network. This discussion painted the picture as to the current state of the GSM attack surface. The GSM protocol stack

is a communications protocol stack like any other. There are many layers of protocols, headers, TLV's, length fields that can "accidentally" be longer or shorter than the actual content. There are timers and state machines. Wrong messages can trigger invalid state transitions. This protocol stack inside the telephone is implemented in C language on the baseband processor on a real-time operating system without any memory protection. This flaw means that the attack surface is increased; especially, because of OpenBSC. OpenBSC is a tool that is freely available that can be used for GSM protocol hacking.

a. ~~(S//NF)~~ (U//FOUO) **Analysis.** GSM networks have, for the most part, been off limits for attackers (phreakers) historically speaking. With the release of these freely available GSM protocol tools (OpenBSC), the avenues for attacking GSM has greatly increased. This could be a precursor for a security nightmare on the GSM network. Expect to see more attacks on the GSM network in the near future.

b. ~~(S//NF)~~ (U//FOUO) **Countermeasure.** Enforcing OPSEC and INFOSEC training is a must. As the GSM network can be attacked by anyone not only for eavesdropping, but for denying service. Consider using secure Iridium phones whenever practical.

9. **(U) "Yes We Can't!" – on kleptography and cryptovirology.** What is kleptograhpy and cryptovirology? Kleptography (the art of employing public key cryptography maliciously as part of a malware attack, such as in ransomware) and the related cryptovirology (the art of embedding cryptographic Trojans inside tamper-proof cryptosystems). During this talk Dr. Moti Yung discussed some of the realities of these threats. He didn't go into detail of how to employ the two, but he did underscore the security threat that the two malicious attacks can present. This is an instance where something that was developed to bring security and peace of mind has been manipulated into something that an attacker can use to blackmail and/or attack without much effort.

c. **(U) Analysis.** These two attacks are very serious and can be difficult to attack and remedy. Traditional virus signatures will have a hard time recognizing cryptovirology. Phishing attacks, especially brought on by poor OPSEC and PII practices, can make this attack easier to be conducted.

d. ~~(C)~~ **(U//FOUO) Countermeasure.** Ensure that users are briefed about phishing and spear fishing attacks. Keep virus definitions up-to-date and ensure that email signatures are being utilized within MARFOREUR/AF. At home, do not open email that you do not know the sender. Be weary, if a deal sounds too good to be true, it most likely is.

10. **(U) Black Ops of PKI.** This talk was given by Dan Kaminsky. He is a penetration tester for a security company in the US. He made the case for the insecurity of PKI on the Internet. Mainly, because of the lack of trusted

certificate authorities—it is far too easy to obtain a "valid" certificate. Further, he explained some of the common ways to masquerade as a valid certificate in several different web browsers (Internet Explorer being one). He went on to praise the DoD for having a working PKI system. For the open Internet, he said he had hope in Secure DNS in hopefully curbing the number of invalid/unauthorized certificate authorities. Basically, making it harder to obtain a certificate and making PKI more secure.

a. **(U) Analysis.** Secure DNS will help with the issue of certificate authority on the Internet. It is scheduled to be released within about six months. The current state is that PKI on the Internet should not be considered a means to identify an entity or user is who they say they are. The DoD should continue to implement and secure the PKI CAs to ensure the infrastructure validity.
b. **(U) Countermeasure.** Ensure that users at MARFOREUR/AF are aware that the PKI on the Internet is not the same as PKI within the DoD. It is not secure, so do not trust it like you would at work. Not to say it cannot be trusted, it just needs to be scrutinized more.

(U) Conclusion. The Chaos Communication Congress 26C3 Here Be Dragons conference was a good security conference to attend. It explored the "out-of-band" security issues faced by systems currently employed by the world and specifically, the DoD (MARFOEUR/AF). The conference provided a good means to observe the hacker community in Europe. The talks provided interesting and thought provoking security discussions which can be used to provide awareness at MARFOREUR/AF. From what I gathered, there were no impending direct attacks (hacks) on US Persons or MARFOREUR at the conference.

M. J. HOSBURGH